

INFORMATION SECURITY & PRIVACY NEWS

A Publication of the Information Security Committee
ABA Section of Science & Technology Law

WINTER 2011 VOLUME 2 ISSUE 1

Editor

[Thomas J Shaw, Esq.](#)
Tokyo, Japan

Committee Leadership

Co-Chairs' Message

Co-Chairs:

[David J Navetta](#)
Denver, CO

[Kathryn R. Coburn](#)
Pacific Palisades, CA

Vice-Chairs:

[Benjamin Tomhave](#)
Fairfax, VA

[Peter McLaughlin](#)
Boston, MA

[SciTech Homepage](#)

[InfoSec Homepage](#)

[Join the InfoSec
Committee](#)

© 2010 American Bar Association. All rights reserved.
Editorial policy: *Information Security & Privacy News* endeavors to provide information about current developments in law, information security, privacy and technology that is of professional interest to the members of the Information Security Committee of the ABA Section of Science & Technology Law. Material published in *Information Security & Privacy News* reflect the views of the authors and does not necessarily reflect the position of the ABA, the Section of Science & Technology Law, or the Editor(s).



ABA SECTION OF
SCIENCE & TECHNOLOGY LAW

Cloud Computing Customers' "Bill of Rights"

By [David Navetta](#)

During the course of our firm's work with clients, especially on the customer side, certain "roadblocks" consistently appear which make it very difficult for organizations to analyze and understand the legal risks associated with cloud computing. In some instances this can result in a willing customer walking away from a deal. So we thought it would be a good idea to create a very basic "Bill of Rights" to serve as the foundation of a cloud relationship, allow for more transparency and enable a better understanding of potential legal risks associated with the cloud. While we use the strong term "rights," we know that cloud arrangements vary and that every transaction has its own issues and circumstances that impact the nature and scope [Read more](#)

Full Disk Encryption – An In-Depth Look

By [Robert Jueneman](#)

Encryption is assuming an increasingly important function with the wide-spread use of open networks and shared systems and platforms, such as the Internet and cloud computing. Protecting data residing on disks is one use of encryption technology. The critical aspects of any encryption system include how the encryption keys are generated, protected, and exchanged throughout their life, the encryption algorithm used and the mode of operation. This article will focus on the latter and more technically detailed of those aspects, modes of operation. NIST has published several comprehensive documents which provide detailed technical guidance on encryption. The Modes of Operation are specified in the following NIST documents: [Read more](#)

2010(2H) Information Law Updates – Cases, Statutes and Standards

By [Thomas Shaw](#)

In the second half of 2010, there have been quite a large number of developments in U.S. and international information security and privacy statutes, cases and standards. This includes U.S. state and federal laws and regulations and those laws of other countries that have been passed or coming into force. It also involves civil and criminal cases and enforcement actions brought by regulators. And it encompasses the new standards and guidelines related to information security and privacy. To briefly summarize the major developments in this area of law and practice, each significant development is presented with a brief analysis after it. Deeper analyses of these developments can be found in our committee's forthcoming book, in other articles [Read more](#)

Book Extract – Data Breach and Encryption Handbook

By [Lucy Thomson](#)

Data breaches are increasing at an alarming rate, leading to identity theft and fraud and devastating financial losses and disruption for millions of individuals. They are a manifestation of the crisis in information security that currently threatens governments and business around the world. Organized crime groups and sophisticated international hackers are suspected of being responsible for some of the major breaches. Other data breaches - many of which occurred at major retailers, financial institutions, payment card processors, universities, healthcare providers, law firms and government agencies - were caused by exceedingly lax security that reveals a cavalier disregard for protecting the important client and customer records. [Read more](#)

Cloud Computing Customers' "Bill of Rights"

By David Navetta



During the course of our firm's work with clients, especially on the customer side, certain "roadblocks" consistently appear which make it very difficult for organizations to analyze and understand the legal risks associated with cloud computing. In some instances this can result in a willing customer walking away from a deal. So we thought it would be a good idea to create a very basic "Bill of Rights" to serve as the foundation of a cloud relationship, allow for more transparency and enable a better understanding of potential legal risks associated with the cloud.

While we use the strong term "rights," we know that cloud arrangements vary and that every transaction has its own issues and circumstances that impact the nature and scope of a negotiation. Moreover, as with the real Bill of Rights, we realize that none of these rights are absolute and may appropriately be subject to reasonable limitations in certain contexts. This article should be viewed less as a universal mandate, and more as a tool for cloud customers and providers to engage in spirited debate about the issues addressed in this new cloud computing Bill of Rights.

Cloud Customers' Bill of Rights (Annotated)

Article I – Data Location Transparency

Cloud service providers shall reveal the physical location of the servers that will be processing their cloud customers' data, and shall provide reasonable advance notice if those physical locations change; cloud service providers shall coordinate with their customers to assure compliance with local laws and any applicable restrictions on the transfer of certain categories of data from one jurisdiction to another.

Comments: The bottom line for this right is that in this day and age, for better or worse, the nature of the data and the physical location of its processing dictate legal obligations of cloud customers. Transborder data flow issues are not new, but they are magnified in the cloud context where the free flow of data across borders may be the norm (and this free flow will only increase as the "Intercloud"¹ arises and data processing begins to behave more like electricity).

The classic example is the EU Data Protection Directive.² A company that moves data made up of personal information of EU residents outside of the EU to certain countries (like the U.S.) risks a violation of EU law. In addition, the recent privacy law³ passed by the Canadian province of Alberta prohibits the transfer of Canadian personal information outside of Canada without providing certain

¹ <http://www.helium.com/items/1967022-cloud-computing>

² http://en.wikipedia.org/wiki/Data_Protection_Directive.

³ <http://www.infolawgroup.com/2010/05/articles/breach-notice/faq-on-albertas-new-breach-notice-law/>

notices to the data subject. Another example is the desire for some entities⁴ to avoid having their data processed on U.S. soil because of the USA Patriot Act. The processing of data in an unexpected country might also generally implicate jurisdictional issues⁵ over a particular cloud customer. Finally, in another twist, having to disclose certain data that is subject to a discovery request could run afoul of privacy laws in certain jurisdictions⁶ -- forcing the cloud customer to choose between violating the law and losing their lawsuit if they don't produce the evidence.

Cloud service providers that fail or refuse to reveal where their customers' data is being processed risk exposing their customers to significant regulatory and legal risk. Unfortunately there are some providers that simply refuse to provide this information (either because they don't want to, or perhaps because they don't know or can't keep track of where data is being processed). Other cloud providers are more sensitive to this issue and will actually contractually agree that their customers' data will be processed only in certain countries or locations. Nonetheless, for cloud customers to truly understand the legal risk of the Cloud, they need this information.

Article II -- Security Transparency

Cloud service providers shall provide full information and access to documentation concerning their security policies and measures, including the ability for cloud customers to conduct periodic security assessments and obtain relevant security-related information and documents from the service provider; this information and documentation should address data integrity and availability as well as the confidentiality of customer data.

Comments: Cloud customers may be ultimately liable for security breaches suffered by their cloud service providers. Moreover, cloud customers may have legal obligations to maintain certain security measures. These obligations do not disappear just because a customer's data is being processed by a cloud service provider. Yet, in many cloud transactions, getting good information about security can be very difficult. While many cloud service providers are willing to provide SAS70 reports, if not tied to established data security standards such as ISO 27002,⁷ these reports may provide only a limited picture of security (and often the picture limited to that which the provider desires to reveal). Unless the cloud customer is a large entity (and even then), most cloud providers will not allow for an independent security assessment by the customer. Moreover, in long term relationships, a cloud provider's security stance may change. Even if in-depth information is provided at the outset of a cloud relationship, if security is not allowed to be revisited, cloud customers may be at risk. Similar to the data location issue, this can result in very unpleasant surprises in the form of security breaches,

⁴ <http://www.enterprisestorageforum.com/outsourcing/article.php/3904981/Could-Borders-Bring-the-Cloud-Down-to-Earth.htm>

⁵ <http://www.glggroup.com/News/Who-has-Legal-Jurisdiction-in-the-Cloud--50084.html>

⁶ <http://www.law.georgetown.edu/cleblog/post.cfm/district-court-orders-production-despite-german-data-protection-act>

⁷ http://en.wikipedia.org/wiki/ISO/IEC_27002

lawsuits and regulatory actions. As such, from the cloud customer point of view, transparency around a cloud provider's security is of paramount importance.

Article III -- Subcontractor Transparency

Cloud service providers shall provide cloud customers with notice as to which third parties will have the ability to access customer's data and for what purposes, including subcontractors, subcontractors of subcontractors and so on.

Comments: It is not uncommon for cloud customers to discover that the cloud service provider with whom they are entering into an agreement is not the sole entity that will be processing their data. The classic example is a SaaS running on a third party cloud. These relationships may be more attenuated than meets the eye as there may be third and fourth levels of cloud providers processing customer data, and the cloud customer may have no idea who is actually handling their data. Even if a cloud provider has revealed its subcontractors at the outset, it is not unusual for a cloud provider to switch subcontractors in the middle of a contract term. From the cloud customer's point of view it is important to know exactly who will have access to its data, and whether those entities pose additional risk. Unfortunately, these subcontracting relationships may not be revealed up front by cloud providers, and are even less likely to be revealed in the middle of a cloud relationship. Rather, many cloud contracts contain clauses that provide the service provider with the right to use third parties, or are silent on the issue. As such, some cloud customers may want to impose certain contract conditions to govern the use of subcontractors.

Article IV -- Subcontractor Due Diligence and Contractual Obligations

Cloud service providers shall conduct reasonable due diligence and security assessments of subcontractors or other third parties that will have access to customers' data or systems, and shall enter into contracts with such third parties that hold those third parties to substantially similar obligations as in their cloud agreements with their customers; cloud service providers shall manage and similarly limit the ability of their subcontractors to utilize other subcontractors.

Comments: As a corollary to Article III above, to the extent that cloud providers do utilize subcontractors to process their customers' information, a proper vetting of those subcontractors is appropriate, as well as certain contractual obligations. The providers' due diligence should include not only data security and privacy assessments of their subcontractors, but also more generally ensuring that their subcontractors are capable of carrying out the promises made by the cloud providers to their customers. This due diligence should be buttressed by contractual obligations imposed on subcontractors that match those made by the cloud provider to its customers. Finally, both for their own protection and the protection of their customers, cloud providers need to worry about and limit their subcontractors' ability to use subcontractors further down the line.

Article V – Customer Data Ownership and Use Limited to Services

Cloud customers shall have the right to solely “own” the data they put into a cloud service provider’s cloud, and cloud service providers shall use their customers’ information solely for the purposes of providing services to the customer, unless otherwise explicitly agreed.

Comments: Certain types of data flowing through cloud providers’ systems is extremely valuable (e.g. personal information of users) and there may be some temptation to use or exploit this data (or perhaps it is part of their business plan). Customers will expect that their cloud providers acknowledge that the customers are the sole owners of that data relative to the providers, and that the data should only be used to provide services to the cloud customer. In fact, this was one of the key requirements⁸ of the City of Los Angeles when it agreed to use Google cloud services. If service providers are going to use data beyond the purpose of providing services, prior notice to their customers should be provided. Service providers that do use their customers' data beyond primary purposes risk hurting their customers’ relationships with their clients and customers, and risk rendering their customers in violation of their privacy policies or data privacy laws.

Article VI – Response to Legal Process

Cloud service providers shall provide notice (within hours, not days) of the service of any subpoena or other legal process seeking their customers’ data, and shall assist and cooperate with their customers in responding to such legal process.

Comments: The ability of a cloud customer to understand when the government is seeking their data is crucial for managing legal risk. If a cloud service provider sits on a subpoena or other legal process it could harm the target customer, and hamper its ability to adequately respond to such a request and develop legal positions. Cloud service providers should develop a process for promptly dealing with these requests and providing notice to their customers. In the cloud context, with data potentially distributed across multiple geographically distant data centers, developing an efficient process and information flow may be challenging.

Article VII -- Data Retention and Access

Cloud service providers shall reveal their data search, retention and destruction practices to their cloud customers; and shall develop and enable data search, retention and destruction capabilities in order to allow their customers to implement their own data retention programs, efficiently effectuate litigation holds, and locate, collect and preserve relevant data, including metadata; cloud service providers shall

⁸ <http://www.infolawgroup.com/2010/05/articles/cloud-computing-1/whats-in-googles-saas-contract-with-the-city-of-los-angeles-part-one/>

build in processes and controls that allow for the efficient authentication of data (e.g. accurate time-stamping; metadata; chain-of-custody indicators, etc.).

Comments: Most sophisticated organizations have data retention policies and procedures in place for executing a litigation hold and preserving data. Implementing these policies and procedures internally can be a challenge, and that challenge is magnified significantly in a cloud environments where the customer must rely on a third party, the flow of data is very fluid, and data may be intertwined with the data of multiple cloud customers. In an environment where proper eDiscovery and electronic evidence practices can make or break a lawsuit, the search, retention and preservation capabilities of a cloud provider are very important. Cloud customers will be seeking to ensure their own internal policies can be followed in their cloud provider's environment. On the front end, this requires transparency and the availability of technologies that enable the efficient identification, collection and preservation of data. On the back-end, service providers will be expected to cooperate with and assist their customers with obtaining electronic evidence and responding to electronic discovery requests. As discussed with respect to Article VIII, this may be tricky in the cloud context, especially when it comes to a cloud customer's desire for an independent forensic investigation.

Article VIII -- Incident Response

In the event a cloud provider suffers a security breach, Cloud providers shall provide prompt notice of the security breach to their affected cloud customers, shall coordinate, cooperate and assist their customers with the investigation, containment and mitigation of the breach, and shall allow their cloud customers to conduct their own forensic assessment and investigation of the security breach.

Comments: Similar to issues around litigation holds and data preservation, cooperation and coordination is crucial when a cloud service provider suffers a security breach. Again, it is the service provider's customers whose business will suffer due to a breach, especially if procedures are not in place for the containment and mitigation of a breach. This again requires service providers to provide transparency as to their internal incident response processes so that cloud customers can ensure that their own internal incident response policies match up. Also of significance is the ability of cloud customers to access their service provider's facilities and systems in order to conduct their own forensic security assessment. This is important not only for data preservation, but also for substantive defense issues. Cloud customers need to be able to conduct such assessments to determine what went wrong, whether any laws may have been violated, the defenses that may be available to the company, and who was responsible for the breach. On the latter question, in some cases it may be the service provider who was at fault, which makes getting access an interesting proposition. Moreover, the multi-tenancy nature of cloud computing also poses challenges. Some cloud providers claim that independent forensic assessment is not possible because it could expose the data of the provider's other customers and potentially result in a violation of a non-disclosure agreement. Needless to say this is a very tricky issue.

Article IX – Indemnification and Limits of Liability

Cloud service providers shall engage their customers in meaningful discussions and negotiations around indemnification and limitations of liability arising of security breaches, including consideration of exceptions to limits of liability for security breaches suffered by the cloud service providers.

Comments: The reality on this “right” is that for “commoditized” cloud service arrangements there will often be no or very limited negotiation on terms (terms will often be reduced to clicking “I agree” on a website). However, in other cloud service transactions, where the parties are on more equal ground in terms of bargaining power, these terms are and should be up for negotiation and debate.

From the customer perspective, it is ceding control of some of its most precious assets: its ability to provide its goods or services, and its data. When a customer suffers a breach internally its incentives are to mitigate the breach and potential adverse consequences to the organization. In the cloud context the service provider’s interests may not be aligned with those goals (in fact, to the extent the service provider was at fault, its interests may run counter to its customers’). Service providers, may choose to put their own considerations very high up. Also to the extent a breach involves multiple cloud customers, cloud service providers may also favor the interest of particular customers over others. This lack of control and reliance on the providers justifies serious consideration of indemnification clauses, consequential damages disclaimers and limitations of liabilities. In some cases, service providers may provide higher limits of liability (or even no limits of liability) for confidentiality breaches or security breaches.

David J. Navetta is one of the founding partners of the Information Law Group. David focuses on technology, privacy, information security and intellectual property law. He is also a CIPP. David has enjoyed a wide variety of legal experiences that have provided him with a unique perspective and legal skill set, including work at a large international law firm, in-house experience at a multinational financial institution, and an entrepreneurial endeavor running his own law firm. Prior to co-founding his current firm, David established InfoSecCompliance LLC (“ISC”), a law firm focusing on information technology-related law. He previously worked for over three years as assistant general counsel and was engaged in commercial litigation for several years prior to going in-house, working at a large international law firm. David has spoken and written extensively about the legal risks and issues associated with cloud computing, including numerous publications on his firm’s site:

<http://www.infolawgroup.com>. He is also co-chair of the ABA’s Information Security committee.

Full Disk Encryption – An In-Depth Look

*(Editor's Note: The following is an extract of the essay written by the author for the forthcoming Information Security committee book: *Information Security and Privacy – A Practical Guide for Global Executives, Lawyers and Technologists*. Because of its highly technical subject matter, it is best published here. Extracts from the book will appear in the next issue of the *ISPN*.)*

By Robert R. Jueneman



Encryption is assuming an increasingly important function with the wide-spread use of open networks and shared systems and platforms, such as the Internet and cloud computing. Protecting data residing on disks is one use of encryption technology. The critical aspects of any encryption system include how the encryption keys are generated, protected, and exchanged throughout their life, the encryption algorithm used and the mode of operation. This article will focus on the latter and more technically detailed of those aspects, modes of operation.

The U.S. National Institute of Standards and Technology (NIST) has published several comprehensive documents, called Special Publications (SP), which provide detailed technical guidance on encryption. The Modes of Operation are specified in the following NIST documents: SP 800-38A, SP 800-38C, and SP 800-38E. The modes listed including Electronic Code Book (ECB), CBC (Cipher Block Chaining), CCM (Counter with Cipher Block Chaining-Message Authentication Code), CFB (Cipher Feedback), CTR (Counter Mode), and OFB (Output Feedback Mode).

Recently NIST has published a draft of SP 800-38E, which adds the XTS-AES mode derived from IEEE standard P-1619. It is unlikely that a busy professionals or procurement specialists would have the necessary background or even the interest to dig through these technical details in order to decide for themselves which of these various standards are most relevant, and why. For that reason, it is unfortunate that the NIST publications, such as SP 800-111, do not address this important issue directly. The short answer is that the most preferable Mode of Operation for Full Disk Encryption or sector-based media encryption is the new XTS-AES, with the second most preferable mode being Cipher Block Chaining, or CBC. Electronic Code Book (ECB) mode has some various serious shortcomings, and the other modes are particularly vulnerable and should not be used for sector-based Full Disk Encryption.

Disk Encryption Modes of Operation

As indicated, there are a number of approved cryptographic Modes of Operation, and they may be perfectly valid and usable for certain operations. However, several of these have serious deficiencies when used for sector-based media or Full Disk Encryption, because of the key reuse problem. In general, unique, randomly generated keys, together with a randomly generated, non-repeating Initialization Vector should be used any time a message or piece of text is encrypted, in order to avoid a class of problems called key reuse. This is easily done in the case of file encryption or link encryption.

In the case of sector-by-sector disk or media encryption, however, a single common key is usually used to encrypt an entire disk or volume, or at least a partition. In addition, adding a 128-bit Initialization Vector (IV) would add 16 bytes to each 512-byte sector on the disk, and that in turn would throw off the entire operating system's file management system, since disks have fixed length sectors¹. For that reason, virtually all software Full Disk Encryption systems "cheat," and use an IV that is a function of the logical sector number. That of course violates the rule about not being able to guess or reuse the IV, and it means that if a given sector is reused, at least the first block of 16 bytes could be compromised with a known plaintext attack, and messages that are identical up to a certain point could easily be identified as such. In addition, because a single key is usually used to encrypt the entire disk, key reuse becomes a serious problem. It is therefore important to analyze what are called the Modes of Operation, in order to see how to mitigate this problem.

Of the various Modes of Operation,² Output Feedback Mode (OFB), Counter Mode (CTR), and Counter with CBC-MAC (CCM) all operate similarly. They all generate a string of pseudo-random bits that begins with some starting point (an Initialization Vector, or IV), and that string is then exclusive-ORed (XORed) with the plaintext that is to be encrypted. However, the Initialization Vector is almost always derived from the sector number and therefore never changes, and thus the string of random bits used to encrypt a particular sector is always the same.

Now consider what would happen if an attacker could copy some or all of the encrypted sectors on the device at some initial point in time, and then copy the encrypted data again at some later time. Assuming some of the data has changed, it would be possible to exclusive-OR the two versions of the changed sector together. This would have the effect of cancelling out ALL of the random encryption bits, and leave the XOR of the plaintext strings as a result. Because of the redundancy in any natural language, in most cases it would be a trivial matter to decode such a result, and recover both plaintext strings.

One very simple way to accomplish this would be to contrive to copy the encrypted media shortly after it has been formatted, so that the encrypted results of every sector would be available. Since the unused free space is formatted with a known pattern, the contribution of the encryption operation would be immediately apparent. Then by reading the media after data has been written to it, the encrypted data would be apparent, and the encryption could be undone by XORing the before and after copies, and then XORing the common free space pattern, typically 00's or FF's.

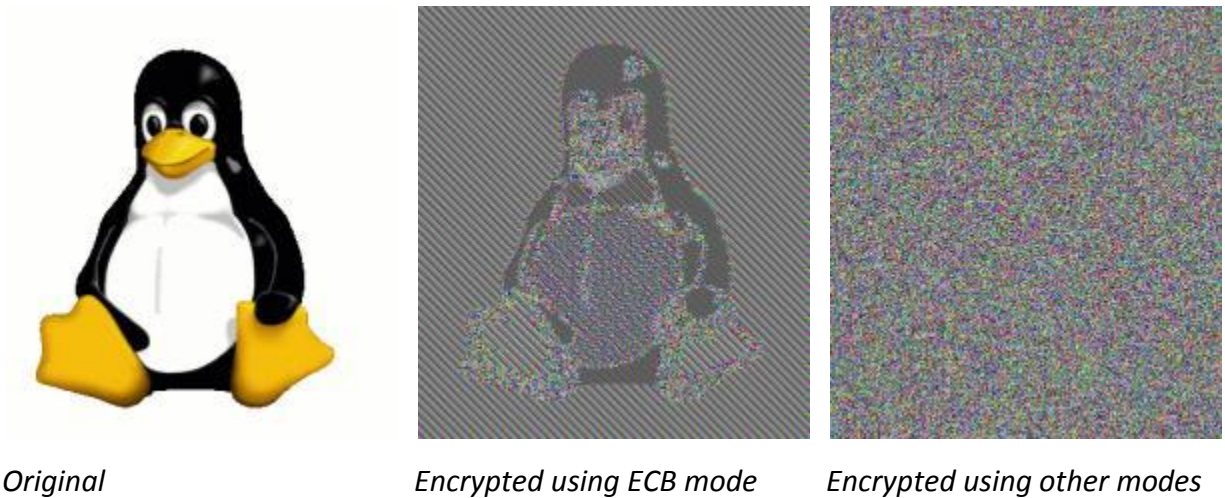
The CCM mode has utility in other contexts because it adds a degree of integrity checking to the encrypted result, but it would share the same problems as OFB and CTR.

¹ Hardware disk encryption systems could conceivably use extended-length sectors to accommodate such an IV, but the use of such an IV would be difficult to manage. To the best of our knowledge, no presently available hardware disk encryption schemes use an extended sector size, or incorporate an IV in each sector.

² See NIST SP 800-38A/38C/38E for a definition of the various Modes of Operation. Also see http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation for an introductory discussion.

Finally, Cipher Feedback (CFB) is generally too slow to be used on a disk, because it only outputs 1 (or sometimes 8) bits per round of the encryption operation. As a result, we can see that OFB, CTR, and CCM modes should not be used for disk or media encryption.

That leaves the Electronic Code Book (ECB) and Cipher Block Chaining (CBC) modes to deal with, in addition to the new XTS-AES mode that was specifically designed to overcome some of these problems.



The Electronic Code Book (ECB) mode is used in several Full Disk Encryption and media encryption products. However, as the above pictures³ make clear, it is far from ideal, because the same plaintext always generates the same ciphertext — there is no mixing or diffusion of information that would make the encryption vary according to the context. Not only can this leak information across files written at different times, it can also leak information within a file, for example if a word or phrase is repeated, or even certain pixels are repeated, as demonstrated above.

Cipher Block Chaining (CBC) was invented specifically to counteract such a threat. It normally uses a unique Initialization Vector to start the encryption, and then chains each block to be encrypted to the previous one. If there is any variability anywhere in the message, that block and all of the subsequent blocks in the message will be completely and randomly different. In its intended application, a random, unpredictable, and unique Initialization Vector is always used for each block of text or message, and the IV must never repeat or be reused within the life of the key.

However, as we have observed, the use of a secret, non-repeating IV for disk or media encryption is impractical, given the fixed length sectors used within virtually all disk drives, even those without rotating memories, such as the NAND-flash based media commonly used in USB “thumb drives.”

³ See http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation)

Another problem concerns what is called a “watermark,” which can be used to prove that a specially created file exists on the disk. The exact method of constructing the watermark depends on the exact function providing the IVs; but the general recipe is to create two encrypted sectors, which have identical first blocks b_1 and b_2 ; these two are then related to each other by $b_2 \oplus IV_2 = b_1 \oplus IV_1$, where the \oplus symbol denotes the Exclusive OR (XOR) operation. Thus, when these two sectors are encrypted, they both encrypt to the same thing, leaving a watermark on the disk. The exact pattern of “same-different-same-different” on disk can then be altered to make the watermark unique to a given file.

More importantly, this scheme might provide a way for malware to covertly exfiltrate some secret information, e.g., a short file, or potentially a file encryption key, in a way that would probably survive most inspection attempts.

To summarize, the CBC mode has a number of problems:

- Copying of CBC mode encrypted sectors to other sectors can result in unauthorized decryption and loss of confidentiality, with the possible exception of the first data block (if the IV is unknown).
- If copying to free sectors is prevented, the attacker can still modify a CBC-encrypted file in place without detection, including insertion of watermarks that are undetected by the owner.
- Sophisticated disk encryption side-channel attacks such as the watermarking attack are aimed at the CBC mode and the vulnerability of the IV to discovery.

For that reason, we can add both ECB and CBC to the list of undesirable Modes of Operation. The solution to these problems is to “tweak” the cipher by adding some variation to the blocks within a given sector, so that the same plaintext encrypted to two different sectors, even using the same key, will result in a completely different output.

The XTS-AES Mode of Operation

On August 17, 2009, NIST released a draft of SP 800-38E for public comment and the final, approved version was released in January 2010. This standard adds the XTS-AES Mode of Operation to the list of FIPS-approved Modes of Operation. The main feature of this family of block encryption algorithms for disk encryption is the use of a sector-based “tweakable” cipher that adds additional security.

A tweakable block cipher inputs a sector-derived input called the *tweak* in addition to the plaintext or ciphertext input. The tweak, along with the key, selects the permutation computed by the cipher so that no two sectors are processed in exactly the same way. This prevents the adversary from decrypting any sector of the disk by copying it to an unused sector of the disk and performing an unauthorized decryption. It also prevents identical plaintext sectors from encrypting to identical ciphertexts (similar to CBC block cipher mode for identical plaintext blocks) and thus leaking potentially useful information to an attacker.

The tweakable block cipher now recommended by NIST and used by several advanced hardware and software-based sector-based disk encryption products is called XTS-AES. Designed by Phil Rogaway in 2003, standardization of this algorithm has been carried out under the IEEE P-1619 “Standard Architecture for Encrypted Shared Storage Media,” December 2007. The extended algorithm is called XTS, for XEX Ciphertext Stealing. The XEX mode is a subset of the full XTS specification that applies in the case of disk sectors that are a multiple of the block size of the encryption algorithm, as of course is the case with the conventional 512-byte sectors used on virtually all disk storage mechanisms

The “tweak” computations involve deriving a secret value by encrypting the sector number with a second AES key, and then extending that value by multiplying it by a Galois polynomial for each subsequent block. The resulting string is then XORed with the plaintext before the encryption (using ECB mode to encrypt each block in turn), and again after the encryption, in order to pre-whiten the input and post-whiten the output⁴. In effect, the text is almost (but not quite) triple-encrypted, using two keys in a manner reminiscent of two-key triple-DES.

The use of XTS-AES prevents all of the problems associated with the other Modes of Operation as described above, by the use of a double-XORed inclusion of sector and block address-specific information into the encrypted file. The copying and modification attacks on AES CBC that are described above cannot occur with an XTS-encrypted sector or drive. Copying or moving an XTS-encrypted block to a different sector offers no advantage to the attacker. Any weakness due to the role of the IV is avoided since no IV is used in XEX. Use of GF (2^N)-based arithmetic, where N is 128, 192, or 256, provides a sound balance of efficiency and resistance to attack that is hard to achieve with other disk encryption algorithms, and greatly surpasses the protection offered by AES CBC by itself.

In summary, XTS-AES is strongly recommended. The ECB, OFB, CTR, CCM, or CFB Modes of Operation should NEVER be used for media or full disk encryption. CBC should only be used if XTS-AES is not available.

Robert Jueneman is the Chief Scientist at SPYRUS, Inc. Mr. Jueneman has been the prime mover of, and intimately involved with the architecture and design of SPYRUS' Cryptographic Modernization initiative for the last seven years, leading to the certification of the SPYRUS Hydra PC product by NSA as the only commercial off-the-shelf file encryption USB product to be approved for protecting tactical SECRET information. Formerly with IBM, Satellite Business Systems, Computer Sciences Corp, the Contel Technology Center, GTE Laboratories, Novell, and President of Jueneman Consulting, LLC, Mr. Jueneman has nearly 50 years of experience in computer and communications, and nearly 40 years of experience in applied cryptography. He is an Associate Member of the ABA, and a prolific contributor to the Information Security Committee within the Science & Technology section of the ABA.

⁴ For a more detailed description, see http://en.wikipedia.org/wiki/Disk_encryption_theory, or IEEE P-1619.

2010 (2H) Information Law Updates – Cases, Statutes and Standards

By Thomas Shaw



In the second half of 2010, there have been quite a large number of developments in U.S. and international information security and privacy statutes, cases and standards. This includes U.S. state and federal laws and regulations and those laws of other countries that have been passed or coming into force. It also involves civil and criminal cases and enforcement actions brought by regulators. And it encompasses the new standards and guidelines related to information security and privacy. To briefly summarize the major developments in this area of law and practice, each significant development is presented with a brief analysis after it. Deeper analyses of these developments can be found in our committee's forthcoming book, in other articles in this publication and in writings by Information Security committee members. While the scope of this article is the second half of 2010, some developments from the first half of this year are also included.

Statutes and Regulations – U.S. Federal

HIPAA - Standards¹

The Office of Civil Rights (OCR) in the Department of Health and Human Services (HHS) has published guidance on risk analysis in *HIPAA Security Standards: Guidance on Risk Analysis*. This covers the risk assessment process that will lead to the information security controls that are used to comply with the HIPAA Security Rule. The risk assessment is a “thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of e-PHI held by the covered entity.”

HIPAA – Privacy, Security and Enforcement Rules²

In July, HHS issued a notice of proposed rulemaking to modify the HIPAA Privacy, Security and Enforcement Rules for changes made by the HITECH Act and some other changes for longstanding HIPAA issues. Some of the major changes to the HIPAA Rules include:

- Adds subcontractors (meaning any agent, even if no contract exists) of Business Associates (BAs) to the definition of “business associate” to the extent that they access protected health information (“PHI”)
- Requires BAs to enter into written contracts with those subcontractors, just as BAs must with Covered Entities (CEs)
- Requires BAs to comply with HIPAA’s privacy and security (administrative, physical, and technical safeguards) requirements for PHI

¹ *HIPAA Security Standards: Guidance on Risk Analysis - Draft*, HHS OCR (2010).

² *Modifications to the HIPAA Privacy, Security, and Enforcement Rules under the Health Information Technology for Economic and Clinical Health Act; Proposed Rule*, Federal Register (July 14 2010).

- Applies the Security and Enforcement Rules penalty provisions directly to BAs (not just through their contracts with CEs)
- Clarifies that a BA is not making a permitted use or disclosure under the Privacy Rule if it does not apply the minimum necessary standard
- Changes HIPAA's privacy and security requirements for PHI
- Limits the processing of PHI to the "minimum necessary" to accomplish the intended purpose, which for now is the limited data set (PHI without direct people identifiers)
- Establishes new limits on the use and disclosure of PHI for fundraising and marketing purposes
- Expands Individuals' rights to access and accountings of PHI disclosures
- Requires CEs and BAs to provide breach notification to Individuals
- Requires BAs to take reasonable steps to cure a material breach
- Prohibits the sale by CEs/BAs of PHI unless a valid authorization is received, with several exceptions (e.g. for public health or research purposes)
- Requires CEs to comply with certain requests from Individuals for restrictions on PHI disclosure
- Revises the requirements for the notice of privacy practices
- Revises the definition of "marketing" in the Privacy Rule
- Protects PHI for up to 50 years after the death of the decedent

HIPAA – Electronic Health Records^{3,4}

In July, the Centers for Medicare and Medicaid Services ("CMS") and the Office of the National Coordinator for Health Information Technology ("ONC") issued two final rules to implement the Electronic Health Records ("EHR") incentive program under HITECH. They are also both working with OCR to address the privacy and security safeguards that result from adopting these rules.

The CMS rule clarifies the specific criteria and objectives that providers must achieve in order to qualify for incentive payments from federal government to ramp up the implementation of a nationwide EHR system. The new final rules on "meaningful use" are intended to provide incentives for both the implementation of EHRs and the use of EHRs to improve safety, quality and efficiency of care. In order to demonstrate "meaningful use" of EHRs, there is a set of "core" criteria and a "menu" of objectives from which providers can choose to comply based upon their particular circumstances.

The ONC rule specifies the particular technical capabilities that EHR technology must meet in order to be certified, and lays out certain procedural steps to be taken in order to obtain such certification. The certification criteria adopted in the final ONC Rule adopts a temporary certification program for health information technology, identifying technical standards which must be met in the certification process, which is a prerequisite to qualification for the HER incentive programs.

³ *Medicare and Medicaid Programs; Electronic Health Record Incentive Program; Final Rule*, Federal Register (July 28 2010).

⁴ *Health Information Technology: Initial Set of Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology*, Federal Register (July 28 2010).

HIPAA – Breach Notification Rule⁵

In August, HHS announced withdrawal of its final rule breach notification for unsecured PHI. One provision that was contentious in the interim rule was the ability of a business to determine if consumers were likely to be at “significant risk for financial, reputational or other harm” for in deciding whether or not to report the breach. HHS intends to publish a final rule in the coming months and until then, the interim final rule remains in effect.

Dodd-Frank Wall Street Reform and Consumer Protection Act⁶

One part of this massive new statute regulating the financial industry, called the “Consumer Financial Protection Act of 2010,” has created a new Bureau of Consumer Financial Protection (the “Bureau”). The purpose of the Bureau is to implement and enforce federal “consumer financial law consistently for consumer financial products and services and that markets for consumer financial products and services are fair, transparent, and competitive.” It will have the authority to create and enforce regulations for financial institutions and those organizations that provide financial products or services. The Bureau will create rules to prevent “unfair, deceptive, or abusive acts or practices” or discrimination. This “unfair and deceptive” standard is used by the FTC when investigating data breaches or the adequacy of organizations’ information security and privacy policies. Combined with the new standard for “abusive acts or practices,” the Bureau has a wider authority to oversee the information security and privacy practices of those providing financial products and services.

SWIFT⁷

In August, the transfer of certain international bank transfer information gathered by the SWIFT system to the U.S. government entered into force. The purpose of allowing the U.S. officials to review this financial information is to identify (and hopefully be able to bring to justice) terrorists and those who back them. This agreement covers transfer to non-EU countries but not transfers within the EU itself. This process is meant to be used to allow bulk transfers of such data until the EU’s own version of a “Terrorism Finance Tracking Program” is in place so that it the EU can do its own analysis of the data without a need for such transfers.

Encryption Export Rule⁸

The U.S. Department of Commerce has published a new interim final rule regarding the export of commercial items related to encryption, such as software or information. These changes include removing items that supported encryption but where encryption was not the primary function of the product and letting mass market encryption products be processed under streamlined rules for items

⁵ See <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/finalruleupdate.html>

⁶ *Dodd-Frank Wall Street Reform and Consumer Protection Act*, Public Law 111–203, July 21, 2010.

⁷ See <http://news.softpedia.com/news/SWIFT-Data-Transfer-Agreement-with-US-Passes-European-Parliament-146985.shtml>

⁸ *Encryption Export Controls: Revision of License Exception ENC and Mass Market Eligibility, Submission Procedures, Reporting Requirements, License Application Requirements, and Addition of Note 4 to Category 5, Part 2; Interim Final Rule*, Federal Register (June 25 2010).

involving use of less sensitive encryption. Examples of the former category includes household appliances, fire alarm systems, robotics and inventory management software and of the latter includes LAN routers and other items that meet the Wassenaar Arrangement mass market criteria.

*CFTC Proposed Rules*⁹

The U.S. Commodity Futures Trading Commission (“CFTC”) has issued two notices of proposed rulemaking, based on the privacy rules of Gramm-Leach-Bliley Act (“GLBA”) and the marketing and data disposal rules of the Fair Credit Report Act (“FCRA”). For GLBA, because the new Dodd-Frank law put two new types of covered entities, major swap participants and swap dealers under the jurisdiction of the CFTC, these two new covered entities become subject to GLBA privacy rules regulating how nonpublic personal information collected from consumers is treated. Under the proposed marketing rule, CFTC-regulated entities that receive consumer “eligibility information” from an affiliate must not market to consumers unless the consumers are notified in advance about the marketing and have a reasonable opportunity to opt-out. The proposed disposal rule would require relevant entities to create and employ written policies and procedures regarding the proper safeguarding and disposal of consumer information they possess or maintain.

*FTC and FCRA*¹⁰

From July, employers who provide payroll information to credit reporting agencies or outsource their payroll or background checks will be subject to FCRA. This includes the ability of an employee to dispute the validity of their data with both the employer who furnished the information and the credit reporting agency. After investigating, an employer must revise any previously furnished incorrect information with the credit reporting agency. Employers also must audit the processes and policies that they use to furnish such information and some are suggested based on the characteristics of the employer.

Statutes and Regulations – U.S. States and International

*Connecticut Data Breach Regulations*¹¹

Connecticut’s Insurance Department issued regulations for its licensed entities to notify the department if there are certain information security incidents involving unauthorized access or loss, including those involving business associates or vendors. This is for those incidents that may have an effect on any resident of Connecticut and includes the remedial actions to assist those affected by the incident. The information is any financial, personal or health information processed by one of the licensed entities, even if the information is encrypted.

⁹ *Business Affiliate Marketing and Disposal of Consumer Information Rules*, Federal Register (October 27 2010).

¹⁰ *Procedures To Enhance the Accuracy and Integrity of Information Furnished to Consumer Reporting Agencies Under Section 312 of the Fair and Accurate Credit Transactions Act; Final Rule; Guidelines for Furnishers of Information to Consumer Reporting Agencies; Proposed Rule*, Federal Register (July 1 2009).

¹¹ *Bulletin IC-25*, State of Connecticut Insurance Department (August 18 2010).

*European Data Retention Directive*¹²

The European Data Retention Directive currently deals with information gathered by telecoms on calls and the period of time that such information should be retained. There is a current effort in the EU to have this directive extended to the internet search engines, in an effort to have information to deal with bad actors such as child pornographers. This could require the search engines to extend the amount of time they retain this data, from at least six months to perhaps up to two years or more.

*European Data Protection*¹³

The EU has released its draft vision for updating the EU data protection regime. While stating that the core principles of the 1995 Data Protection Directive were still valid, several issues posed specific challenges, including:

- Addressing the impact of new technologies
- Enhancing the internal market dimension of data protection
- Addressing globalization and improving international data transfers
- Providing a stronger institutional arrangement for the effective enforcement of data protection rules
- Improving the coherence of the data protection legal framework

The document then lists a series of objectives in pursuing this comprehensive approach, including bringing additional focus on issues like data breach notification, sensitive data protection, children's rights, the right to be forgotten and processing of EU citizens data outside the EU, increasing the use of data protection impact assessments, strengthening the DPAs role and internal DPA coordination, considering applying the Directive to criminal justice matters, working towards convergence of national laws and implementations, encouraging EU certification schemes (i.e. "privacy seals"), clarifying the rules for international data transfers and strengthening the role of the Article 29 Working Party.

*Hong Kong Data Breach Guidance*¹⁴ / *Potential Prohibition on Sale of Personal Information*

The Hong Kong Privacy Commissioner for Personal Data recently issued guidance on how organizations should handle data breaches. While voluntary, it includes describes four steps that organizations should take, including gather of information related to the breach, containing the breach, assessing the risk of harm and consideration of giving notice on the breach. Also, several recent incidents have gotten the Privacy Commissioner to consider proposing a new law make it a criminal offence for companies to sell customers' personal data. First, Octopus Holdings Ltd., whose cards are used like electronic cash to buy train tickets, meals and convenience store products, sold clients' information for HKD 44 million. Second, a survey of local banks showed that the banks have full power to do as they

¹² *Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.*

¹³ *A comprehensive approach on personal data protection in the European Union*, European Commission (Nov. 4 2011).

¹⁴ *Guidance on Data Breach Handling and the Giving of Breach Notifications*, Office of the Privacy Commissioner for Personal Data, Hong Kong (2010).

please with personal information provided by credit card applicants. The credit card application forms have no "opt-in" or "opt-out" clauses with regards to privacy matters and they admit using personal data for purposes other than conducting credit checks and collecting debts. The lack of opt-in and opt-out clauses violates the Personal Data (Privacy) Ordinance, which requires companies to provide the option of not receiving further promotional information.

New Zealand Cross-Border Information Law¹⁵

In September this new law went into force, giving the Privacy Commissioner in New Zealand the power to stop transfers of personal information out of the country by issuing a transfer prohibition notice. This is to protect the situation where New Zealand is used as an intermediary for data transferred out of countries that view its privacy protection program as sufficient and then transferred again on to a country whose privacy protections may be inadequate. "Inadequate" are those safeguards that are "not comparable" to those in New Zealand and would violate the OECD privacy principles.

Australian Privacy Principles¹⁶

In June, the government released its direction for updating the Privacy Act of 1988. The Australian Privacy Principles (APPs), combine and enhance the Information Privacy Principles for government agencies and the National Privacy Principles for private sector organizations. One proposed APP changes the focus from data that leaves the country to data disclosed outside the country, such as by a third party outside Australia dealing with data inside the country. Another addresses direct marketing and requires consent for use of sensitive information and allows for opt-out for non-sensitive personal information. There are requirements for a "clearly expressed" privacy policy and expanded details in privacy notices. Future releases will address the areas of health information and credit reporting.

Mexico Data Protection Law¹⁷

In July, the Federal Law for the Protection of Personal Data in Control of Private Persons came into force for private companies in Mexico, even for non-Mexican citizens. Much like the EU, this law broadly requires consent before personal data of the data subjects is processed. Consent can be obtained if there is no objection to data notices, except for sensitive data, where express consent must be obtained. It requires notice when personal information is collected and that it only be used for the stated purpose. Data subjects must be able to access and correct their own information and appropriate safeguards must be put into place, not of a lower standard than those used by the data processors themselves. Data processors should be accountable for any violation of the principles and data breaches having certain impacts require immediate notification to the data subjects. Cross-border data transfers of personal information may occur with notification. Personal information must be deleted if no longer required for the purpose indicated on the privacy notice.

¹⁵ New Zealand, *Privacy (Cross-border Information) Amendment Act 2010*, Public Act 2010 No 113.

¹⁶ Australia, *Australian Privacy Principles*, Exposure Draft (2010).

¹⁷ United Mexican States, *Federal Law on Protection of Personal Data Held by Private Parties* (2010).

Cases – Civil and Criminal

Flash Cookies Cases

There have been a number of lawsuits filed recently regarding the use of online cookies to track consumers' browsing habits and the consumers' lack of awareness of and inability to prevent such tracking. These lawsuits follow a report¹⁸ that found that more than half of the 100 top websites sampled are using Adobe Flash cookies to store information about visitors, and that some of these are also using Flash cookies to re-initiate cookies that were deleted by consumers. Flash cookies differ from HTML cookies in that they are stored in a different location and are not blocked or deleted by privacy controls on browsers in the way HTML cookies are. They also can contain up to 100k of data versus 4k for HTML cookies. The Flash cookie can be used to also bring back an HTML cookies that was deleted (a "zombie" cookie), without providing notice to, or obtaining consent from, the consumer by storing the same information in the Flash cookie. Flash cookies are not managed by browser cookie privacy controls, rather, users must delete them using either Adobe controls or browser add-ons. While Flash cookies have a legitimate purpose for retaining users' preferences for Flash-based applications, here they are not being used as such and are defeating user attempts to prevent tracking. In the privacy policies of the surveyed websites, very few disclosed the use of Flash cookies.

*Valdez v. Quantcast*¹⁹

This lawsuit, as did the others, targets both the company who generate the "re-spawned" cookies (Quantcast) and the media affiliates (e.g. ABC, ESPN, NBC, MTV) who utilize this service for their websites. The lawsuit alleges that the companies using this technology violated federal laws such as CFAA, ECPA, the Video Privacy Protection Act and state laws by using Flash storage to re-create HTML cookies deleted by users and so tracker user's movement across the Internet without their knowledge or consent, including on sites not affiliated with Quantcast. In doing so, personal, personally identifiable and/or sensitive information of consumers was obtained with their consent. The media defendants also allegedly do not identify the use of flash cookies for tracking purposes in their website terms of use or privacy policies. Quantcast privacy policy allegedly states that Flash cookies are "used only for audience measurement and not behavioral ad targeting" and requires "college level reading skills for comprehension."

*Aguirre v. Clearspring Technologies*²⁰

This lawsuit alleges that Clearspring and a series of media companies (e.g. Disney, Warner Bros.), violated the CFAA and state law by tracking the web movements of their users, including children, without permission. Clearspring makes the AddThis tool, which enables users to share links via e-mail or social-networking sites. Clearspring set Flash cookies on users' computers so that they could access their online activities, including sites not affiliated with Clearspring. They also allegedly re-spawned

¹⁸ *Flash Cookies and Privacy*, A. Soltani, S. Canty, Q. Mayo, L. Thomas, C.J. Hoofnagle, Univ. Cal., Berkeley, Aug. 10, 2009.

¹⁹ *Valdez v. Quantcast Corporation, et. al.*, Case No. 2:10-cv-05484-GW-JCG (C.D. Cal 2010).

²⁰ *Aguirre v. Clearspring Technologies, Inc., et. al.*, Case No. 2:10-cv-05948-UA-DUTY (C.D. Cal 2010).

“zombie” cookies and did not disclose this in their privacy policy. The suit alleges that data was obtained by tracking users when they accessed the Internet from different computers, at home and at work. The information collected sensitive information may include such things as users' such as “gender, age, race, number of children, education level, geographic location, and household income” and may have included the items purchased, documents read and personal and financial information.

*Aquirre v. Quantcast*²¹

This class action suit for violation of the CFAA and state laws was brought against both Quantcast and Hulu, as the “Internet audience metrics company” and a streamer of video content respectively. This was for introducing a “cookie-like tracking code” on the user computers when visiting the Hulu site. This was in the form of the Flash cookie described above. The use of this Flash cookie was used to circumvent the information security and privacy controls on the users’ computers. With this exploit, two defendants allegedly acquired personal information and were able to track consumers as they utilized the Internet, all without the knowledge or consent of the users.

*La Court v. Specific Media*²²

This class action lawsuit was initiated against Specific Media, Inc. alleging that it violated the CFAA as well as state laws. The suit again cited the use of Flash cookies to recreate deleted browser cookies. Allegedly, Specific Media violated users’ “privacy, financial interests and computer security rights” by storing tracking codes in Flash cookies, in order to “re-spawn” HTML cookies after users intentionally deleted the HTML cookies. The complaint alleges that Specific Media re-created the HTML cookies so it could obtain personally identifiable and sensitive information, monitor online activity, and sell users’ data. As with the other suits as well, the complaint asserts that Specific Media’s privacy documents are “deceptive by design” and “sufficiently vague.” The use of Flash cookies is discussed only for audience measurement and not for behavioral ad-targeting and the opt-out option is inconspicuous.

*Intezkostas v. Fox*²³

This lawsuit accuses Fox Entertainment Group and the American idol.com website, along with Clearspring of using flash cookies in the manner described in the cases above, in violation of the CFAA and state laws.

*Aughenbaugh v. Ringleader Digital*²⁴

This suit claimed that Ringleader Digital, a mobile ad technology company, and its media affiliates (e.g. CNN, Travel Channel, Merriam-Webster), violated the plaintiffs’ privacy through the use of local HTML 5 mobile browser databases to track mobile devices uses. The complaint alleges that the company and

²¹ *Aquirre v. Quantcast Corporation, et. al.*, Case No. 2:10-cv-05716-GW-JCG (C.D. Cal 2010).

²² *La Court v. Specific Media, Inc.*, Case No. 8:10-cv-01256-JVS-VBK (C.D. Cal 2010).

²³ *Intezkostas v. Fox Entertainment Group, et. al.*, Case No. CV10-6586 (C.D. Cal. 2010).

²⁴ *Aughenbaugh v. Ringleader Digital, Inc., et. al.*, Case No. 8:10-cv-01407-CJC -RNB (C.D. Cal. 2010).

its affiliates intentionally exploited the operating software on the plaintiffs' mobile devices and tracked their mobile activity for ad purposes without permission. Ringleader's Media Stamp "software contains local storage databases that allow Web sites to store information on these devices, which when used appropriately enhance internet browsing on mobile devices." The suit claims that even if users can find the HTML5 database and delete it, it is simply recreated with the same identifying information. "This is clear evidence of the Defendants attempts to further thwart the efforts of mobile device users to protect their privacy."

*Browser Compact Policies*²⁵

In a related issue but not (yet) a case, researchers at the Carnegie Mellon University have found that a large number of websites have invalid compact privacy policies. These type of policies allow third party cookies to be placed on computers using Internet Explorer, even though the browser is set to reject them. It utilizes P3P codes used only by this browser, but not Firefox, Chrome or Safari, to check what a website's privacy policies. If there are not enough or invalid codes in the compact privacy policy, Internet Explorer will let the cookies be installed. The paper also notes that 134 sites with TRUSTe seals, which are meant to reassure consumers that strong privacy measures are in place at a Web site, have faulty compact policies. Only 391 of over 3,000 sites with the seal had compact policies at all.

Social Networking Site Privacy Cases

The following cases are some of the first to deal with the issue of whether there is a right of privacy for data on social networking sites when a discovery request is made for information on those sites. These cases are further explored in the forthcoming book from the ABA's Information Security committee: *Information Security and Privacy – A Practical Guide for Global Executives, Lawyers and Technologists*.

*Crispin v. Christian Audigier*²⁶

In this case, the defendant wanted to view the communications of the plaintiff on the plaintiff's social networking sites, Facebook and MySpace. But the court, after ruling that these social networking sites were both remote computing service ("RCS") providers and an electronic communication service ("ECS") providers under the Stored Communications Act (SCA), held that these types of entities are required not to disclose the defendant's communications via email that are "inherently private." For those communications that the plaintiff has made available only to certain approved users on his Facebook wall or MySpace comments, these cannot be disclosed under the SCA. If the privacy settings are for public access, then the SCA does not restrict protect these from discovery. The key here was this was a third-party discovery subpoena, not a direct request to the party for information they control that is posted on their social networking sites.

*EEOC v. Simply Storage Management*²⁷

²⁵ *Token Attempt: The Misrepresentation of Website Privacy Policies through the Misuse of P3P Compact Policy Tokens*, CMU CyLab, Leon, Cranor, McDonald, McGuire (2010).

²⁶ *Crispin v. Christian Audigier, Inc. et. al.*, Case No. CV 09-09509 MMM-JEMx (C.D. Cal. 2010).

The court held that the "locked" and "private" portions of the social networking accounts of two individuals claiming to have suffered severe emotional distress were relevant to their claims. The court found that posts, profiles, photographs, and videos relating to the plaintiffs' mental states were relevant and therefore discoverable, and ordered that they be disclosed. The court also noted that because this information was already shared with others on the social networking site, it tends to dilute their privacy arguments.

*Romano v Steelcase*²⁸

The defendants claimed that to mount an effective defense, they would need to have access to the plaintiff's posting on her social networking sites. As she claimed permanent injuries that caused her to not be able to partake in certain activities, the defendants wanted to be able to review her private postings on the sites. This was after reviewing the public part of the sites and finding her engaged in activities that she claimed that she was no longer able to partake in. The court ruled that material on the private part of her site is likely to be relevant and should be discoverable. The court also ruled that posting on a social networking site by their very nature are to share them with others, so it would be difficult to sustain a claim to a reasonable expectation of privacy.

*McMillen v. Hummingbird Speedway*²⁹

Defendants sought access in discovery to the plaintiff's social networking sites, to ascertain whether he made any statements contradicting his allegations of possible permanent impairment. After reviewing the public portion of his website and finding such statements, defendants filed a motion to compel. The plaintiff asked that his communications among private friends be considered confidential and therefore privileged against discovery. The court reviewed the privacy policies of the Facebook and MySpace social networking sites the plaintiff belonged to. These policies discussed disclosures on other users' home pages, even after deleting an account, as well as disclosure for legal reasons, to avoid bodily harm or other harm to the user or the social networking company and would of course be disclosed to the website's operators. As such, there can be no reasonable expectation that any communications would remain confidential, as in an attorney-client or priest-penitent relationship nor is there any requirement for friendships to maintain confidentiality.

*NLRB v. American Medical Response of CT*³⁰

In a separate type of case involving social media, an employee was fired for criticizing her employer is to have a hearing in January before the National Labor Relations Board (NLRB). The company's employee handbook had a blogging and Internet posting policy, which stated that "Employees are prohibited from making disparaging, discriminatory or defamatory comments when discussing the

²⁷ *Equal Employment Opportunity Commission v. Simply Storage Management LLC*, 2010 WL 3446105 (S.D. Ind. 2010)

²⁸ *Romano v Steelcase, Inc.*, 907 N.Y.S.2d 650 (N.Y.Sup. 2010)

²⁹ *McMillen v. Hummingbird Speedway, Inc.*, No. 113 – 2010 CD (Jefferson County, PA 2010).

³⁰ *American Medical Response of CT, Inc. and International Brotherhood of Teamsters, Local 443*, NLRB Case No. 34-CA-12576.

Company or the employee's superiors, co-workers and/or competitors.” The NLRB charged that such policies interfere with employee’s rights under section 7 of the National Labor Relations Act³¹ “to engage in protected concerted activity” (talking with their co-workers about jobs and bosses), even if is unrelated to union activity.

*West Coast Detail & Accessory Centre and United Food and Commercial Workers Union*³²

In this case from Canada involving social media, two employees were fired for making “damaging comments” about their employer’s business and “very offensive, insulting and disrespectful comments” about their managers. These comments were made on Facebook, to a total of almost 500 Facebook friends, many current or former employees of the company. In the hearing before the British Columbia Labour Relations Board (BCLRB), the court ruled that the employees could have no “serious expectation of privacy” on this social networking site. This was in spite of the fact that the company did not have a social networking policy. The court ultimately ruled that the comments on Facebook were “offensive and egregious” and “very egregious” and provided proper cause for the terminations.

*Gould v. Facebook*³³

This lawsuit against Facebook alleges violated state laws and its own privacy policy by sharing users’ personally identifiable information with advertisers. It alleges that Facebook forwards “referrer headers” to advertisers whenever users click on a displayed ad, which can be used to users’ profiles and obtain personal information such as name, gender, and hometown without users’ consent. This problem was raised in a paper³⁴ which the plaintiff forwarded to Facebook. The complaint alleges that despite this notice, Facebook failed to change its practices and has made misleading statements on the sharing of its users’ personal information. The complaint asserts a number of claims, including violation of state unfair competition and computer crime statutes, common law breach of contract, and common law negligence. This case has now been consolidated with another similar case.³⁵

CFAA Cases

There have been several similar cases involving CFAA claims and proving harm above the statutory limit. The CFAA defines “loss” as any reasonable cost “including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.” It must be in excess of \$5,000 in a one-year period.

A Ohio federal court held that the cost of investigating ways to make a website more secure after an authorized access into the website constitutes “loss” to meet the \$5,000 jurisdictional amount, as this

³¹ *National Labor Relations Act*, 29 U.S.C. § 157.

³² *West Coast Detail & Accessory Centre and United Food and Commercial Workers Union Local 1518*, BCLRB No. B190/2010.

³³ *Gould v. Facebook, Inc.*, Case No. 10-cv-2389 (N.D. Cal. 2010).

³⁴ *On the Leakage of Personally Identifiable Information Via Online Social Networks*, B. Krishnamurthy and C.Wills (2009).

³⁵ *Robertson v. Facebook, Inc.*, Case No. 5:10-cv-02408-JF, (N.D. Cal. 2010).

was a cost of responding and restoring, to the offense.³⁶ A Washington State federal court held that the plaintiff failed to produce evidence showing the \$5,000 jurisdictional amount. The plaintiff claimed that the defendant stole his thumb drive and disseminated documents on the thumb drive over the Internet. The plaintiff claim of loss involved the work that must be done to determine what files were copied from the thumb drive and stored on other computers. The court found that this claim of loss for examining others' computer systems and deleting misappropriated files is "outside the CFAA."³⁷ A Texas federal court held that a claim of lost profits was not sufficient. The defendant's unauthorized access to the plaintiff's website and realty database on multiple occasions without payment of license fees was a sufficient claim under the CFAA but lost profits can only constitute loss under the CFAA when the lost profits are "incurred because of interruption of service."³⁸

There were also two cases decide involving the meaning of "unauthorized access" under the CFAA. A former Goldman Sachs programmer allegedly took source code from a proprietary software trading system when he left his employment with the firm. A New York court held that "'accesses a computer without authorization' and 'exceeds authorized access' cannot be read to encompass an individual's misuse or misappropriation of information to which the individual was permitted access."³⁹ A California court dismissed a CFAA claim for similar reasons. An employee who had fabricated an illness to have time off to work for a competitor and at that time downloaded corporate documents⁴⁰ The court said that although the firm would have removed the access had it known of the deception, the "relevant inquiry is whether the employer allowed the employee use the computer system, irrespective of whether the employer would have revoked permission if it understood the employees' intent, or knew about the employee's conduct." Other federal courts have reached different results.

*Florida v. Certegy*⁴¹

The Florida Attorney General's office settled its enforcement action against Certegy Check Services Inc. after a data breach potentially affecting millions of individuals. Certegy provides authorization of checks. A former employee of Certegy allegedly stole and sold records to a data broker, which included bank account information, credit card numbers and expiration dates, and consumer identifying information such as name, address, and telephone number. The company agreed to pay a large fine and to support education programs plus implement and maintain a comprehensive information security program, to get annual independent audits and to comply with the PCI DSS standard. Certegy had previously settled a class action suit based on the breach.

*Shlahtichman v. 1-800 Contacts*⁴²

³⁶ *Jedson Engineering, Inc. v. Spirit Construction Services, Inc.*, 2010 WL 2541619 *19 (S.D. Ohio June 18, 2010).

³⁷ *Doyle v. Taylor*, 2010 WL 2163521 (E.D. Wash. May 24, 2010).

³⁸ *Costar Realty Information, Inc. v. Field*, 2010 WL 3369349 *14 (D. Md. August 23, 2010).

³⁹ *U.S. v. Aleynikov*, Case No. 10 Cr. 96 (S.D.N.Y. 2010).

⁴⁰ *Accenture, LLP v. Sidhu*, Case No. C10-2977 (N.D. Cal. 2010).

⁴¹ In the matter of *Certegy Check Services, Inc. et al.*, Fla. Case No. L07-3-1109, (2010).

⁴² *Shlahtichman v. 1-800 Contacts, Inc., No. 09 4073* (7th Cir. Aug. 10, 2010).

The U.S. Court of Appeals for the Seventh Circuit clarified merchants' obligations to protect credit and debit card information under FACTA, holding that although it prohibits the printing of certain payment card information on receipts, it does not apply to email confirmations. FACTA prohibits merchants who accept credit or debit cards from "print[ing] more than the last 5 digits of the card number or the expiration date on a receipt provided to the cardholder at the point of sale or transaction. The plaintiff, after making a purchase, received an automated email confirmation containing his credit card's expiration date and subsequently filed a lawsuit, alleging that the inclusion of a payment card expiration date in an email confirmation violated FACTA. The court concluded that an email confirmation is not a "printed" receipt.

*Google Buzz Privacy Litigation*⁴³

Google recently settled a class action lawsuit alleging that its social networking feature, Buzz, violated users' privacy. Buzz was automatically added to all users of Gmail, turning users' frequent e-mail contacts into followers. The users' information and followers were also made public by default, including photos and information shared in other Google products. A putative class action lawsuit was filed, alleging violations of the ECPA, SCA, CFAA and state law. Under the terms of the settlement, the company will "undertake wider public education about the privacy aspects of Buzz." Google also acknowledged that the company has addressed privacy issues, while the plaintiffs agreed that privacy threats no longer exist. Google agreed to create a settlement fund, which will go toward "existing organizations focused on Internet privacy policy or privacy education."

*Hammond v. Bank of New York Mellon*⁴⁴

A putative class action lawsuit against the Bank of New York Mellon for the loss of backup tapes containing personal information was dismissed. The court held that an increased risk of identity theft is not sufficient injury for standing and that the plaintiffs failed to show that they suffered any actual harm as a result of the tape loss incident. As is cases decided elsewhere (many of which are listed in the decision), the mere exposure of personal information is not an adequate basis for a lawsuit until there is some actual harm to the plaintiffs.

*Ruiz v. Gap*⁴⁵

A federal appeals court upheld a dismissal of this case on the grounds that the mere risk of identity theft is too speculative of an injury to substantiate a cause of action based on negligence. The plaintiff had submitted an online job application to work in a Gap store. Subsequently a laptop was stolen from a contractor used by Gap for this online service, containing unencrypted information on almost 1 million job applicants, including the plaintiff. The plaintiff filed a class action suit. The court held that an increased risk of identity theft did not constitute "the level of appreciable harm necessary to assert a negligence claim under California law." The court held that while the increased risk of identity theft

⁴³ *In Re Google Buzz User Privacy Litigation*, Case No. 5:10-CV-00672-JW (N.D. Cal. 2010).

⁴⁴ *Hammond v. The Bank of New York Mellon Corp.*, Case No. 1:08-CV-06060 (S.D.N.Y. June 25, 2010).

⁴⁵ *Ruiz v. Gap, Inc.*, No. 09-15971, 2010 WL 2170993 (9th Cir. May 28, 2010).

created sufficient real threat of future harm to grant plaintiff standing, the alleged injury was still too speculative to sustain a negligence claim. "The negligent act is not accountable unless it results in injury." The courts also held that the breach of contract claim against the subcontractor was properly dismissed, because such a claim requires a showing of "appreciable and actual damage" and none was produced by the plaintiff. The court held that the invasion of privacy claim required an actual violation, not an increased thereof. Finally, the court did not allow the violation of the state's Social Security number protection law, because it covers only the logging into a website, not any subsequent requests for the number after login.

*American Pharmacies v. CVS Caremark*⁴⁶

Six independent pharmacies in Texas filed a lawsuit against CVS Caremark, charging it with racketeering under the federal RICO law, trade secret misappropriation and violations of the HIPAA privacy rule. The suit alleges privacy violations that started only months after the CVS Caremark agreed to pay a large fine and institute corrective action plans following a federal government investigation of potential HIPAA violations. The suit alleges that CVS Caremark is violating a FTC-mandated firewall between its community pharmacy and pharmacy benefit management business units by using by collecting and analyzing patient data for marketing and other purposes in violation of the privacy rule.

*U.S. Copyright Group lawsuits*⁴⁷

Numerous lawsuits have been filed by filmmakers against alleged people who have downloading movies using peer-to-peer network. With their IP addresses, the suits against John Does requiring the tie from the IP address to the actual person. In an effort stop their ISPs from disclosing their names, several of the ISP subscribers sought to quash subpoenas served on the ISP for that purpose. But a federal judge has denied these requests, ruling that the subscribers Web users can't quash subpoenas to their ISPs because subscribers don't have a "cognizable claim of privacy in their subscriber information." The court reasoned that users have no reasonable expectation of privacy in their data because "they already have conveyed such information to their Internet Service Providers."

*City of Ontario v. Quon*⁴⁸

The Supreme Court issued a unanimous decision in this case concerning a public employees' privacy rights in communications performed on employer-issued communications devices. The Court held that the city's review of text messages on a police officer's city-issued pager was reasonable where the city was concerned that, among other things, it might be paying for employees' personal use of those pagers. The Court noted that regardless of the employee's expectation of privacy, an employer's search of an employee's property at work is reasonable if it is a non-investigatory, work-related search and if the search is "justified at its inception" and "reasonable in scope." Because the city had a legitimate

⁴⁶ *American Pharmacies, et. al. v. CVS Caremark Corporation, et. al*, Case No. 6:10-cv-78 (S.D. TX 2010).

⁴⁷ See for example: *ACHTE/NEUNTE BOLL KINO BETEILIGUNGS GMBH & CO. KG v. DOES 1 - 4,577*, Civ. Action No. 10-453 (RMC) (D.D.C. 2010) and *West Bay One, Inc. v. Does 1 - 1,653*, Civ. Action No. 10-481 (RMC) (D.D.C. 2010).

⁴⁸ *City of Ontario v. Quon*, 560 U.S. _____ (2010).

interest in ensuring that it was not paying for personal messages, the Court found that the search was justified at its inception. The Court found that the search was reasonable in scope because it was an “efficient and expedient” way to reach the city’s goal, was not “excessively intrusive,” since it covered only two months’ worth of messages and did not include messages sent or received during non-work hours and the plaintiff did not have much—if any—expectation in privacy in a work-issued pager, because he could reasonably expect that his work-related communications might be subject to scrutiny.

Cases – Regulatory (FTC/FCC/HHS)

*Twitter*⁴⁹

The micro-blogging service Twitter agreed to settle charges with the FTC regarding its privacy and data security practices. The FTC’s complaint had alleged it had failed to provide reasonable security practices, contrary to the company’s website promises to protect user’s personal information. Twice in 2009 intruders obtained control of Twitter administrative accounts because of its deficient password security policies. Unlike the typical FTC case involving information security practices, Twitter does not collect financial information or engage in e-commerce sales of goods. The terms of the settlement requires Twitter not to mislead consumers about the extent to which it protects nonpublic consumer information. As is typical in these settlements, Twitter must maintain a comprehensive risk-based information security program, name a person to be in charge of the program and have periodic independent audits of this program.

According the FTC, Twitter failed to prevent the unauthorized administrative control of its system by not taking “reasonable’ steps, such as:

- Requiring employees to use hard-to-guess passwords
- Prohibiting employees from storing administrative passwords in plain-text in their personal e-mail accounts
- Suspending administrative passwords after a reasonable number of unsuccessful login attempts
- Providing an administrative login page separate from the ordinary user login page and whose location is known only to authorized users
- Enforcing periodic changes of administrative passwords
- Restricting access to administrative controls to employees whose jobs required it

EchoMetrix^{50,51}

The FTC had charged that EchoMetrix, who provide a service that monitors children’s online activity, with deceptive practices in violation of section 5 of the FCT Act. The complaint alleged that

⁴⁹ *In the Matter of Twitter, Inc.*, FTC File No. 0923093, Agreement Containing Consent Order.

⁵⁰ *FTC v. EchoMetrix, Inc.*, Complaint for Permanent Injunction and Other Equitable Relief, Case No. CV10-5516 (E.D.N.Y 2010).

⁵¹ *FTC v. EchoMetrix, Inc.*, Stipulated Final Order for Permanent Injunction and Other Equitable Relief, Case No. CV10-5516 (E.D.N.Y 2010).

information collected from the Sentry parental control software program was made available to third party marketing companies through the Pulse program without adequate notice to the users of the Sentry service. Pulse services “aggregates, collects, measures, or analyzes data from user-generated digital content (including but not limited to Internet forums, message boards, chats, blogs, and instant message conversations) for use by third parties.” The “vague” notice provided to consumers was deep inside a very small scroll box under the end user license agreement. The settlement requires the company to not share the information collected by the Sentry program and to destroy any information already transferred to the Pulse program.

*Verizon*⁵²

The FCC agreed to a consent decree with Verizon Communications after the company had reported a failure of its databases to track customers who had opted out of "customer proprietary network information" ("CPNI") marketing. Verizon said it discovered a discrepancy in the total number of customers in its opt-out database. Verizon agreed to a compliance plan to ensure future compliance with the CPNI opt-out procedures. The Compliance Plan obligates Verizon to perform validation tests, check for transaction errors, enhance its employee training procedures and add CPNI compliance to its management processes.

Spokeo^{53,54}

The Center for Democracy & Technology (CDT) submitted a complaint to the FTC alleging that the data broker website Spokeo was not taking adequate safeguards to protect consumers. Spokeo is a website that allows users the ability to look up "people-related information from phone books, social networks, marketing lists, business sites, and other public sources." According the CDT's complaint, Spokeo violates the FCRA, which requires consumer reporting agencies to take certain actions to protect consumer privacy, including allowing consumers the right to access information about themselves, to correct mistakes and to be advised of adverse decisions made based on Spokeo's data. It also alleges that Spokeo's actions amount to unfair and deceptive acts under the FTC Act. Additionally, a class-action lawsuit has been filed against Spokeo. According to the complaint, Spokeo publishes largely inaccurate and false information about the plaintiff and had marketed this information to employers at a time when the plaintiff was seeking employment.

Rite Aid^{55,56}

Rite Aid agreed to a million-dollar settlement with the U.S. HHS. Rite Aid was accused of violating HIPAA's privacy requirements by improperly disposing of prescriptions, labeled pill bottles and unused labels in their regular trash. Rite Aid is also required to enter into a resolution agreement with HHS

⁵² *In the Matter of Verizon*, FCC File No. EB-09-TC-228, Adopting Order.

⁵³ *In the Matter of Spokeo, Inc.*, Before the FTC, Complaint and Request for Investigation, Injunction, and Other Relief.

⁵⁴ *Robins v. Spokeo, Inc.*, Case No. 2:10-cv-05306-ODW-AGR (C.D. Cal. 2010).

⁵⁵ Rite Aid Resolution Agreement with HHS (June 7 2010).

⁵⁶ *In the Matter of Rite Aid, Inc.*, FTC File No. 072 3121.

under which the company agreed to "implement a strong corrective action program," that includes establishing policies and procedures for disposing of protected health information, creating a training program for handling and disposing of patient information, conducting internal monitoring and getting an independent assessment of its compliance for three years. Rite Aid also was accused by the FTC of violating the FTC Act by failing to implement reasonable and appropriate measures to protect customers' personal information against unauthorized access when it represented in its HIPAA and other disclosures that it would do so. The FTC settlement requires Rite Aid to establish a comprehensive information security program designed to protect the security, confidentiality and integrity of the personal information it collects from consumers and to obtain every two years for the next 20 years an independent, outside audit of that program.

*Novartis*⁵⁷

The FDA told Novartis in a recent letter that its widget for the leukemia drug Tassigna violated FDA advertising rules in part because the widget lacked information about potential health dangers. In response, the drug maker pulled the widget, which allowed Facebook users to share their experiences with the drug. The FDA said that the widget needed to be approved. While Novartis might resolve issues regarding risks and claims with proper disclaimer language embedded in the widget, it would be more difficult, given the unstructured nature of social media, to control users' comments on its pages that might be construed as testimonials.

*Lime Wire*⁵⁸

The FTC has closed its investigation into Lime Wire, who provides both a free and purchasable version of P2P software. The investigation focused on a security vulnerability in legacy versions of the P2P software that put users at risk of inadvertently sharing sensitive information stored on their computers. Among the factors considered as part of closing the investigation were:

- Lime Wire's incorporation of safeguards into the updated software's user interface to help users avoid the inadvertent sharing of sensitive documents;
- the high attrition rate for legacy versions of the software;
- Lime Wire's inability to force users to update to a newer software version; and
- users of some of the older software versions may have been able to avoid disclosure of sensitive PII (noting that an act/practice is not "unfair" under Section 5 unless it causes consumer injury that is not reasonably avoidable by consumers).

*US Search*⁵⁹

The FTC reached a settlement with online data broker US Search on complaints that the company failed to deliver on promises that it would not share the records of customers who paid a fee. US Search, which advertises itself as the top people search website in the U.S. and compiles public records

⁵⁷ NDA # 022068, HHS Letter to Lisa Drucker, Director (July 29 2010).

⁵⁸ *In the Matter of Lim Wire LLC*, FTC File No. 082-3046, Letter to George Searle CEO (August 19 2010).

⁵⁹ *In the Matter of US Search, Inc.*, FTC File No. 1023131.

and sells data about consumers, offered to "lock" the records of customers who paid a US\$10 fee, so that other people using the service could not see or buy the records. But according to the complaint, US Search's PrivacyLock service did not block consumers' names from showing up as an associate of someone else, did not block consumers' information from appearing in a reverse search of their phone numbers or addresses, and did not work if the consumers changed addresses. Under the settlement, US Search must refund the fees paid by customers to have their records locked and not make misrepresentations about the effectiveness of any service that promises to remove information about consumers from its website.

*XY.com*⁶⁰

The founder of a lifestyle website filed for bankruptcy, listing among his assets the names and personal information of the users of his firm's website. The potential sale of this information to satisfy creditors caught much national attention and drew a letter from the FTC. The website had information on upwards of 1,000,000 subscribers, including many young people. The FTC letter states that the sale or transfer of sensitive personal information to a new owner that occurs as part of a bankruptcy proceeding must be in accordance with the privacy policy of the bankrupt entity⁶¹ or the sale would be considered a deceptive business practice, in violation of section 5 of the FTC Act. The privacy policy of the website stated "Please note our amazing privacy policy. We never give your info to anybody." The sale or transfer could also be construed as an unfair business practice under section 5, even to a third party buyer who knew it violated the privacy policy. Referring to its prior *ToysMart* case, the FTC allowed the transfers "where the line of business of the new owner would be substantially similar to that of the old owner, the new owner would abide by the terms of the original owner's privacy policy, and the new owner would obtain affirmative consent from consumers for any material changes to that policy." Due to the age of some of the data and its potential use not being consistent with the purpose of its collection, the FTC believed that it is best that the data is destroyed.

Standards and Guidelines

*PCI DSS*⁶²

The Payment Card Industry Security Standards Council (PCI SSC) has released the revised standards for the PCI Data Security Standard (PCI DSS) and Payment Application-Data Security Standard (PA-DSS). The PA-DSS details what a payment application must support to facilitate a customer's PCI DSS. The revisions to PCI DSS v2.0 were categorized as additional guidance, evolving requirements or clarifications and include:

- Ensuring that all locations of cardholder data are include in the scope
- Providing guidance on virtualization
- Clarifying the key management process

⁶⁰ Letter from FTC's Bureau of Consumer Protection (July 1 2010).

⁶¹ See 11 USC § 363(b) regarding the use, sale, or lease of property in bankruptcy.

⁶² Payment Card Industry Data Security Standard, *Requirements and Security Assessment Procedures* v2.0.

- Using a risk-based approach to vulnerabilities
- Clarifying secure boundaries between Internet and card holder data environment

*GPEN*⁶³

The FTC recently joined with the privacy authorities from eleven other countries to launch the Global Privacy Enforcement Network ("GPEN"). The purpose of this network is to promote cross-border information sharing and enforcement of privacy laws. GPEN has unveiled its new website designed to educate the public.⁶⁴ The GPEN website provides guidelines and how government agencies interested can participate. GPEN's direction includes:

- sharing information about privacy enforcement issues, trends and experiences
- participating in relevant training and cooperating on outreach activities
- engaging in dialogue with relevant private sector organizations
- facilitating effective cross-border privacy enforcement in specific matters

*Security Industry Association Privacy Rules*⁶⁵

The group (SIA) is an industry organization for the electronic physical security industry, including manufacturers, distributors and integrators. Electronic physical security includes devices for biometrics, close circuit TV and RFID. For that audience, end-users and governments writing legislation on this topic, SIA has issued a set of privacy principles that includes the use of privacy impact statements, legal compliance assessments, building in privacy controls, adequate protection of databases holding personally identifiable information and between any components sharing that data, notice of and limits on data collected, breach notification and response and data retention and destruction policies.

*Smart Grid Cyber Security Strategy and Requirements*⁶⁶

The Smart Grid presents certain information security and privacy concerns. For privacy, the Smart Grid significantly increases the amount of data that can be monitored, collected, aggregated and analyzed. In response to these concerns, in August NIST released updated guidance in a non-version of the *Smart Grid Cyber Security Strategy and Requirements*. The three-volume includes a risk assessment framework and security requirements (volume 1) and privacy issues (volume 2). The privacy section has been significantly expanded from the second draft issued in February, including legal frameworks and considerations and has two privacy-related appendices, "Privacy Use Cases" and "Privacy Related Definitions."

*National Strategy for Trusted Identities in Cyberspace*⁶⁷

⁶³ See <http://www.ftc.gov/opa/2010/09/worldprivacy.shtm>

⁶⁴ See www.privacyenforcement.net

⁶⁵ *Privacy Framework*, Security Industry Association (2010).

⁶⁶ NIST IR 7628 v 1.0, *Smart Grid Cyber Security Strategy and Requirements* (2010).

⁶⁷ *National Strategy for Trusted Identities in Cyberspace - Creating Options for Enhanced Online Security and Privacy*, Obama Administration (2010).

The administration issued this document to lay out a vision for an “online environment where individuals, organizations, services, and devices can trust each other because authoritative sources establish and authenticate their digital identities.” It contains four goals and nine actions. The goals are the establishment of a comprehensive identity ecosystem framework, building an interoperable identity infrastructure that implements the framework, enhancing confidence by privacy protections and increasing willingness to participate and ensuring the long-term success of the ecosystem. The actions are include public/private efforts to achieve these goals, enhancing privacy protections, developing both risk models and interoperability standards, addressing liability concerns and international collaboration.

*Protecting Consumer Privacy in an Era of Rapid Change*⁶⁸

The FTC has just released its proposed privacy framework. It composes three major elements, which were drawn from the Privacy Roundtables previously discussed here. Companies should:

1. Promote consumer privacy throughout their organizations and at every stage of product and service development, incorporating substantive privacy protections (e.g. data security, reasonable collection limits, sound retention practices, and data accuracy) and maintaining comprehensive data management procedures throughout the product and service lifecycles.
2. Simplify consumer choice when collecting and using consumers’ data, offering it at a time and in a context in which the consumer is making a decision about his or her data, including its presentation and a special choice mechanism for online behavioral advertising (Do Not Track).
3. Increase the transparency of their data practices, making privacy notices clearer, shorter, and more standardized; providing reasonable access to consumer data; providing prominent disclosures and obtain affirmative express consent before using consumer data in a materially different manner; and helping to educate consumers about commercial data privacy practices.

Thomas J. Shaw, Esq. is an attorney at law, CPA, CIPP, CRISC, CISM, ERM^P, CFF, CISA and CGEIT based in Tokyo, Japan who works with corporations in Asia and globally, on information law (data privacy, information security, e-discovery/litigation readiness), Internet law (cloud computing, social networking, e-commerce, intellectual property), international transactional law, compliance, information governance and litigation and technology risk assessment and management. He is the editor of the forthcoming committee book, Information Security and Privacy – A Practical Guide for Global Executives, Lawyers and Technologists. He is the editor of the EDDE Journal from the ABA’s e-Discovery and Digital Evidence committee. His recent publications have also appeared in the International Law News, SciTech Lawyer, the IAPP’s Privacy Advisor, the Asia Law News and the Law Technology News. He can be reached via email at thomas@tshawlaw.com and on the web at www.tshawlaw.com.

⁶⁸ *Protecting Consumer Privacy in an Era of Rapid Change – A Proposed Framework for Businesses and Policymakers*, Preliminary FTC Staff Report (December 2010).

Book Extract – *Data Breach and Encryption Handbook*

(Editor's Note: This book is the first of three consecutive books to be published by members of the Information Security committee in the first half of 2011 and extracts of each will be featured in these pages. The next issue of ISPN will feature Information Security and Privacy – A Practical Guide for Global Executives, Lawyers and Technologists (a project worked on by many members of our committee). The following issue will feature Cloud Computing – A Practical Guide for Lawyers.)

By Lucy L. Thomson



Data breaches are increasing at an alarming rate, leading to identity theft and fraud and devastating financial losses and disruption for millions of individuals. They are a manifestation of the crisis in information security that currently threatens governments and business around the world. Organized crime groups and sophisticated international hackers are suspected of being responsible for some of the major breaches. Other data breaches - many of which occurred at major retailers, financial institutions, payment card processors, universities, healthcare providers, law firms and government agencies - were caused by exceedingly lax security that reveals a cavalier disregard for protecting the important client and customer records.

With the objective of developing solutions to prevent data breaches, the *Data Breach and Encryption Handbook* addresses the problem of escalating data breaches and its legal ramifications. It focuses in great depth on the law and its implications, encryption technology, recognized methods of resolving a breach, and many related aspects of information security. This book is designed to enable attorneys and technology professionals to understand the root causes of the security failures that lead to many of the massive data breaches so that the practitioner will ask the right questions to address the issues raised by data breaches and how to prevent them. To better illustrate the complex challenges of data breaches, the book examines a number of the major data breach incidents from a variety of legal and technology perspectives; instructive graphics help pinpoint the methodologies hackers used to cause each of these breaches. It consists of 19 chapters in five sections: I – Crisis in Information Security; II – Anatomy of the Major Data Breaches; III – Law; IV – Technology; and V – Response.

Part I – Crisis in Information Security

Alarming Trends -- The past five years has seen a dramatic increase in the number of data breaches reported publicly. Data breaches in the U.S. rose almost 50 percent in 2008. Data breaches in 2010 are up – more breaches have been reported in the first three quarters of 2010 than were reported in 2009. According to Identity Theft Resource Center (ITRC) reports, in 2009 only six of 498 breaches reported that they had either encryption or other strong security features protecting the exposed data. Equally small numbers were reported for 2008, when the ITRC declared that “It is obvious that the bulk of breached data was unprotected by either encryption or even passwords.”

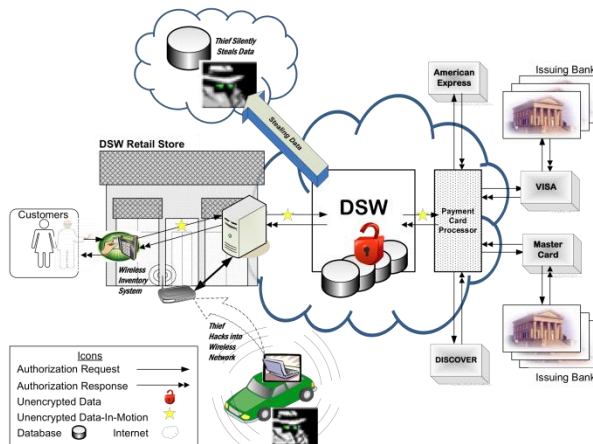
The largest data breaches ever were reported in 2007, 2008 and 2009. The massive data breaches involving Hannaford, Heartland, RBS WorldPay and TJX compromised the personal records of 81,300,000 individuals, potentially exposing them to identity theft and fraud. These numbers are staggering. Of the five industry sectors, the largest number of data breach *incidents* – more than 40 percent -- occurred in the business sector. Hackers have targeted retailers and payment card processors because of the high value for identity theft of the consumer information collected and maintained by these entities. At the same time, business executives have failed to address the multitude of vulnerabilities in their networks, making them prime targets for hackers to exploit.

Millions of Medical Records Were Breached – Healthcare breaches have increased from 13 percent in 2009 to 26.4 percent in 2010. 148 of the 561 U.S. companies and organizations that endured a significant data breach in the first three quarters of 2010 were healthcare providers. Among the top ten largest breaches reported for 2009, health care organizations accounted for half of them. Medical identity theft is a particularly devastating event for individuals whose medical records have been stolen. In light of the government initiatives to create electronic health records for every American by 2014, these breaches illustrate starkly the challenges ahead for policy-makers and health care providers.

Part II – Anatomy of the Major Data Breaches

Encrypted Records -- Failed Security -- It is widely assumed that if sensitive records are “encrypted,” they will be safe. This is the premise underlying a number of the state data breach notification laws, and the new federal breach law for health records (HITECH), which require notification to consumers in the event of a data breach of “unencrypted” records. However, information security is only as good as the weakest link. Data breaches have occurred even where sensitive records were “encrypted” at some point in the information lifecycle. As a result, millions of consumer records have been stolen and individuals have been exposed to risks of identity theft and fraud. This handbook looks behind the statistics and at the security of eight companies that suffered major data breaches. A close look at the root causes of security failures in the major breaches reveals that even if implemented, encryption does not always protect sensitive records -- other critical security controls must also be in place.

One of those breaches is shown in the diagram below. Hackers gained access to the DSW computer networks through wireless access points on the networks. Intruders intercepted wireless signals and connected wirelessly to in-store networks without authorization. The illustration below shows that security “failed” at multiple points, including the use of a wireless system that could be hacked, and storing the sensitive customer information in unencrypted files that could be easily accessed using a commonly known user ID and password.



Behind the Scenes of the DSW Breach

The important protection provided by encryption, however, should not be minimized. When computers, laptops, backup tapes, thumb drives, cell phones, PDAs and other devices with encryption are lost or stolen, encryption is a critical factor in protecting personal records from unauthorized access. Going forward, in addition to encrypting records, individuals and organizations must also devise strategies to ensure that these devices are not lost, stolen or otherwise compromised so that no breach occurs.

Part III – Law

Ambiguities in Security Breach Notification Statutes -- During the past several years there has been a nationwide rush to enact laws and regulations that impose an obligation on businesses to *disclose* security breaches involving personal information to the persons whose data was compromised. Most of these laws do not impose a duty to provide security for that data. Instead, they typically require only that companies disclose security breaches to affected persons.

Taken as a group, the state and federal security breach notification laws generally require that any business in possession of certain sensitive personal information about a covered individual must disclose any breach of such information to the person affected. The laws are generally similar in structure, approach, content and terminology. The key requirements of the breach notification laws vary from state to state, and several have become controversial.

- *Type of Information* -- The sensitive personal information covered by the breach notification laws is typically defined as information consisting of: (1) a person's first name or initial and last name, plus (2) any one of the following: social security number, drivers license or state ID number, or financial account number or credit or debit card number (along with any PIN or other access code where required for access to the account).

- *Definition of breach* – Generally the statutes require notice to affected individuals following the unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality or integrity of personal information about such individuals. In some states, however, notice is not required unless there is a reasonable basis to believe that the breach will result in substantial harm or inconvenience to the affected individual.
- *Who must be notified and when must notice be provided?* -- These vary by state.
- *What Is Encrypted Data?* -- Most of the breach notification statutes provide an exemption if the data is encrypted. That is, notification of data subjects is not required if the security breach involved encrypted data. The manner in which the statutes address the encryption issue, however, varies widely.

Part IV – Technology

Five chapters of the book address encryption; overall they seek to demystify encryption by first identifying it as a basic scientific concept that has existed for thousands of years. Leading encryption experts then explain what encryption really is, what encryption keys are, and how the pieces of the encryption puzzle fit together. For attorneys and security professionals with a more complete understanding of information security, one chapter discusses how encryption can be circumvented or undermined by poor security practices. Another chapter provides an inside look into the future of encryption by the developer of the self-encrypting hard drive. Here are some excerpts.

About a decade ago, when I was consulting with Phoenix Technologies, a small group of us concluded that hard disk drives were, in fact, the best end-point for security and privacy. The motivation for this was the Chernobyl virus that had infected the pre-boot of many hundreds of thousands of PCs. We decided that disk drives were a better place for security precisely because they were in fact complete computers but with strict limits on the code that could run on them. Furthermore, disk drives are where all data is stored. A disk drive (flash drive, etc.) can act as any standalone computer can act. It can protect itself.

So, after completing the BIOS security work for Phoenix Technologies, I wrote a proposal at the end of 2001 to Seagate Technology to put security into disk drive. The stated goals were ubiquity, utility, and uniqueness -- to put security on every disk drive (hard disk drive, flash drive, optical drive, etc.) in the world, achieve clear usefulness and ease of use, and a unique grade of security.

On behalf of Seagate, I led the effort to standardize self-protecting, self-encrypting disk drives in the Trusted Computing Group (TCG). It is now a published standard approved by every major disk drive maker in the world, and developed for optical drives and flash drives with inputs from

the major producers of those devices as well. Nearly every disk drive maker has publicly announced self-encrypting disk drives based on the TCG Storage Workgroup standards.

As the Internet and computing has proliferated, more and more people have come to believe that the information in their computers is their property. We are entering an age of information property, or what I have called “infropery.” This makes it natural that all data, in the future, will have data protection layered on it. The Self-Encrypting drive is a step in that direction.

Self-protecting, self-encrypting, disk drives will be ubiquitous in a few more years. The reason is not just the standard, but that the other two goals, utility and uniqueness, are also achieved by self-encrypting disk drives. Our experience is that self-encrypting disk drives are game changers. This includes both opportunities and challenges for United States and International laws, enforcement, and adjudication particularly in the areas of e-discovery and digital evidence, as well as changes in how we view data privacy and ‘infropery.’

Part V – Response

The *Data Breach and Encryption Handbook* will have accomplished one of its goals if it generates discussion and debate about the best approaches to preventing data breaches. This includes an assessment of whether the state data breach notification laws and HITECH address the real problem – maintaining the security of sensitive personal information – or simply focus on the aftermath of a broken system. The goal of legislation (state, federal and international) should be to prevent data breaches rather than to enact complex and costly requirements that provide little assistance to individuals after their information has been compromised through breaches that result from failed security. Many questions arise as others are answered, among them: Do the state and federal data breach laws facilitate the development of appropriate solutions to prevent data breaches? Does encryption prevent data breaches?

Lucy L. Thomson, J.D., M.S., CIPP/G, is a Senior Principal Engineer and Privacy Advocate at CSC, a global technology company. She works on teams building modernized information systems, and has developed strategies to safeguard sensitive information at the nation’s ports, as well as for the government’s key financial systems. Appointed Consumer Privacy Ombudsman in eleven of the largest federal bankruptcy cases, she has overseen the disposition of 125 million electronic consumer records. A career U.S. Department of Justice litigator, Ms. Thomson served in senior positions in the Criminal and Civil Rights Divisions and pioneered the use of electronic evidence at trial. She is Vice Chair of the ABA Section of Science & Technology Law, and serves in the ABA House of Delegates. She founded and co-chairs the ABA e-Discovery and Digital Evidence (EDDE) and Homeland Security Committees, and is editor of the Data Breach and Encryption Handbook (2011) and the Symposium on Homeland Security in Jurimetrics: The Journal of Science and Technology (2007).

Committee Co-Chairs' Message

Dear ISC Members:

Hello everybody and welcome to another issue of *Information Security and Privacy News*. We are now proudly starting the second year of this publication and look forward to many more years of great articles written by and for our members. It is your contributions that make this a strong and informative publication, so please add to your New Year's resolutions a plan to submit at least one article for publication in the *ISPN* during 2011, on any topic related to information security and privacy.

There are many things going on with the ISC now and in the first quarter of next year, as follows.

As many of you know, our committee's book, now titled *Information Security and Privacy – A Practical Guide for Global Executives, Lawyers and Technologists*, has gotten through the final editing process and so we expect publication after the first of the year. This essentially new book targets the three audiences described in its title but we are also trying to break new ground in getting this book distributed to not only to non-lawyer audiences but also to those outside the U.S. market. We will be making various efforts to market this book at the RSA conference and in other forums. Committee members are encouraged to pass the word among their professional contacts and at conferences.

On January 25 at 13:00 EST, we will be hosting a live audio webinar and teleconference titled "Hot Topics in Information Security Law." The panel will be providing the most recent information on a number of topics, including the status of data security legislation, at the federal, state and international levels. They will also be looking at regulators and enforcement and litigation involving the various data breaches, such as involving payment card data security breaches, consumer data breaches and online banking security breaches. The ISC has begun a working group dedicated to helping legislators with policy issues and developing data security legislation. The panel will also cover cloud computing and social networking and their impacts on information security and privacy. Here is the link to the program. <http://www.abanet.org/cle/programs/t11hts1.html>

On February 12-13, the committee will be having a pre-RSA meeting in San Francisco. This meeting, for which we will also try to provide remote and time-delayed access, will include discussions on Securing Medical Devices and Security in the Cloud. More information and additional topics will soon follow. This meeting will be held in the law firm offices of Foley & Lardner LLP. Please add this to your calendar and plan on attending in person if you will be going the RSA conference afterwards.

That is it for now. Please keep your eye out for new announcements concerning these upcoming meetings. Until then, see you on the list-serve and on the web. Have a happy and safe holiday season.

David Navetta
ISC Co-Chair